

SECTION 5.4 OFFENDER ACCESS TO COMPUTERS

TABLE OF CONTENTS

5.4.	Offender Access to Computers.....	2
5.4.1.	Information.....	5
5.4.1.1.	Offender Citrix Environment (OAC Network)	5
5.4.1.2.	Non-networked PC's.....	5
5.4.2.	Types of access.....	5
5.4.2.1.	Inmate access to computers for employment purposes.....	5
5.4.2.2.	Inmate access to computers for educational and legal purposes	5
5.4.3.	Viewing of legal material provided on an external storage device (e.g. CD, DVD, MP3, USB flash drive)	5
5.4.4.	Supervision	6
5.4.5.	Electronic supervision.....	6
5.4.6.	Network printers – CSI workplaces.....	6
5.4.7.	Software.....	7
5.4.7.1.	Inmate purchase of software.....	7
5.4.7.2.	Software register.....	7
5.4.7.3.	Software - OAC Network.....	8
5.4.8.	Disks.....	8
5.4.8.1.	Inmate disk register	8
5.4.8.2.	Distance Education/External Education programs.....	9
5.4.9.	Transfer of data between PC's being used by staff and those being used by inmates	9
5.4.10.	Reporting of infringements.....	9
	OFFENDER COMPUTER SECURITY CHECK	10

5.4. Offender Access to Computers

Summary Page

Policy Overview	Offender participation in effective programs to reduce the risks of re-offending is a goal of the CSNSW Corporate Plan. This includes increasing the skill levels of inmates.
Purpose	• To outline the circumstances under which offenders may have access to desktop computers for authorised education and / or training purposes and / or work activities. (Note: Inmates cannot have access to laptop computers in any setting). This includes the practical supplementation of theory classes and distance learning studies and in the case of CSI activities, practical application for administrative functions. • To establish a corporate policy that recognises the importance of offender's access to computers, while developing a regulated framework, that recognises and manages the security compliance of that access. • To detail correctional centre staff responsibilities for the security, storage and audit of all educational and business unit hardware and software held at a centre. • To detail correctional centre education staff responsibilities for intranet and internet use for educational purposes and correctional centre staff use of CSI Business Management System centres (Pronto) (CSI-BMS) in conjunction with the CSI Policy Manual. • To outline the relevant procedures to be followed for offenders purchasing software. • To identify correctional centre staff responsibilities when offenders use desktop computer and other technological equipment. • To outline offender responsibilities with regards to the use of technology equipment and desktop computers.
Scope	This policy applies to all General Managers, (delegate), Industries Managers, Senior Correctional Education Officers (SCEO) and qualified personnel who work within correctional centres and places of detention where educational and/or vocational training programs and work programs are provided (Refer to Scope of work activities, S8.8, (2), CSI Policy Manual). The CSI Policy Manual should be consulted for specific policy concerning employment of inmates. That manual includes information concerning inmate access to computers in the course of their employment that must be read with this policy. These procedures affect all staff working within correctional centres.
Strategic Focus	• Corporate Plan 2009-2012: Offender Management
Legislation	• <i>Crimes (Administration of Sentences) Act 1999</i> • <i>Crimes (Administration of Sentences) Regulation 2008</i>
Related Policies	OPM • section 9.3.1.1 - Legal Documents

- section 9.1.2 – Approved private property
- section 9.8.17 – Education, Art & Craft Materials

CSI Policy Manual

- section 8.6 – Security within Correctional Industry Programs
- section 8.6.2 – Maintenance of Security
- section 8.6.5 – Contraband and Searches
- section 8.8 – Inmate involvement in clerical work

ACO/SACD 99/107, 2004/052

DCOMO 2012/26

**Commissioner's
Memorandum** 05/14

Definitions

AEVTI	Adult Education and Vocational Training Institute
CSI	Corrective Services Industries
CSI - BMS	Corrective Services Industries – Business Management System (Pronto)
Antivirus / virus protection	A software program that checks for and rectifies desktop computer viruses.
Exempt Body	• the Ombudsman • the Commonwealth Ombudsman • the Judicial Commission • the National Crime Authority • the New South Wales Crime Commission • the Anti-Discrimination Board • the Police Integrity Commission • the Commonwealth Human Rights & Equal Opportunity Commission • the Independent Commission Against Corruption • the Privacy Commission • the Legal Aid Commission • the Legal Services Commissioner • the Legal Services Tribunal • the Administrative Decisions Tribunal
Exempt Person	• a Member of Parliament • a legal practitioner • a police officer
Freeware	Freely distributed desktop computer software that does not incur fees of any kind.
Hardware	The physical components of a desktop computer system e.g. the central processing unit (the desktop computer box), the keyboard and the screen.

Industries Manager	Operations Manager, Manager of Industries, Business Unit Manager, Manager of Centre Services & Employment, Principle Industries Officers, Chief Industries Officers, Manager of Offender Services, Manager of Offender Services and Programs
Information technology peripherals	Devices such as colour printers, scanners, digital cameras, cd writers and other removable storage devices.
Modem – modulator/ DE modulator	A device that permits the dispatch and receipt of data along a telephone line.
Prosecutorial bodies	NSW Police, Australian Federal Police, NSW Director of Public Prosecutions, Commonwealth Director of Public Prosecutions and the Police Services and Directors of Public Prosecutions of the remainder of the States and Territories of Australia not already listed above.
Senior Correctional Education Officer (SCEO)	In the case where there is no senior correctional education officer, the correctional education officer and/or a delegated member of correctional centre AEVTI staff.
Shareware	Freely distributed desktop computer software that incurs a nominal licence fee after a fifteen- to forty-five-day trial period.
Software	The programs or instructions that control the working of a desktop computer. System software controls access to disk drives, printers and so on, and also controls the running of other programs. Application software is designed to carry out particular tasks such as word processing, page makeup, disk conversion and virus detection. For the purpose of this policy, software means individual disks, and complete software packages on floppy disks or CDs.
Supervision	in the context of this policy means: • Continuing operational awareness and implementation of the policy requirements. • Formal assessment and continuing monitoring of the appropriateness of individual offenders having access to desktop computers (including reference to the Corrections Intelligence Group) and execution of the <i>'Guidelines for Offenders Using Computers'</i> (Annexure 5.6). • Regular physical and electronic supervision of offenders in accordance with a risk assessment to ensure the requirements of this policy are met.
Supervising Officer	Can be the Industries Manager, SCEO, correctional officer, correctional education officer, or a teacher.
Virus	A program that interferes with the regular functioning of a desktop computer. The presence of a virus may not be readily apparent to the user, although symptoms such as the slowing of responses to commands or unexpectedly altered screen displays often indicate that something is wrong.

Work disk	A floppy disk, containing course material, supplied with a distance learning course. A work disk is also a blank floppy disk supplied by a correctional education officer for education and training purposes.
------------------	--

5.4.1. Information

This policy concerns inmate access to computers for work, educational and legal purposes.

Staff must also consult the *CSI Policy Manual* for specific information concerning employment of inmates. That manual includes information concerning inmate access to computers in the course of their employment that must be read with this policy.

All personal computers (PC's) for the use of inmates are identifiable through their colour – green. There are some authorised exceptions to these, being some PC's located with CSI and Education areas.

5.4.1.1. Offender Citrix Environment (OAC Network)

The CSNSW Offender Citrix Environment was rolled out in 2011. Referred to in this policy as the Offender Access to Computers (OAC) Network, it is a solution designed and deployed to support user access from correctional centres.

The OAC Network is a centralised network, allowing inmates to maintain their work regardless of their location. Each green computer is preloaded with a set of software applications and allows each inmate who has an OAC Network account, to login to the OAC Network and save their work to their own 'My Documents' folder on a central server, enabling them to access their work from different green PC's at different locations.

5.4.1.2. Non-networked PC's

There will remain some PC's for the use of inmates that will not be part of the OAC Network. Non OAC Network PC's will include stand-alone green computers for inmates to view and prepare legal documentation and at some remote CSI locations which do not need to be part of the OAC Network.

5.4.2. Types of access

5.4.2.1. Inmate access to computers for employment purposes

The procedures for inmate employment as a CSI/AEVTI clerk are outlined in the *CSI Policy Manual*. The balance of this policy concerns inmate access to computers for educational and legal purposes.

5.4.2.2. Inmate access to computers for educational and legal purposes

All inmates seeking access to desktop computers for educational purposes or to access a computer to view and prepare legal documentation are required to fill out the following forms:

- *Inmate Application for Access to Computers - Annexure 5.5*
- *Guidelines for Inmates Using Computers – Annexure 5.6*

Inmates are to not have access to a laptop computer for any purpose.

5.4.3. Viewing of legal material provided on an external storage device (e.g. CD, DVD, MP3, USB flash drive)

Staff must only accept and allow access by an inmate to their legal material supplied on an external storage device that have been sent by an inmate's legal representative, an exempt body or a prosecutorial body. The external storage device must be supplied with a

letter from the inmate's legal representative, the exempt body or the prosecutorial body stating that the contents of the external storage device contain material pertinent to the inmate's case. The external storage device must be recorded on a private property receipt and booked into the inmate's property through the OIMS Inmate Property module (refer section 9). The inmate must be provided a copy of the letter so that they are aware of the receipt of the legal material. The inmate can then attend the Inmate Property Store to gain access their legal material (refer section 9 for further details about management of inmate property).

Staff are not to view the contents of external storage device containing legal material that has been supplied, with a supporting letter, by an inmate's legal representative, an exempt body or a prosecutorial body, as the contents would be considered privileged.

Exempt and Prosecutorial bodies are listed above in the definitions section.

5.4.4. Supervision

Inmates must be subject to regular supervision in classroom and work areas when using computers. An officer may monitor an offender's computer use by direct supervision, CCTV or by logging into CITRIX to covertly shadow an offender's session.

Electronic supervision must also be carried out as detailed below.

Prior to an inmate commencing using a PC that is part of the OAC Network, the supervising officer shall ensure that the cables connecting the computer to the network are connected to the correct computer and network ports.

When conducting regular supervision either directly or by CCTV, the supervising officer must ensure that:

- a) inmates are only using the desktop computer assigned to them; and
- b) inmates are not attempting to tamper with the desktop computer software, hardware or cabling;

5.4.5. Electronic supervision

Electronic supervision refers to checking of computer drives and inmate files (inmate folders on the computer system) for non-authorised files including non-authorised software. A thorough check must be carried out monthly.

To undertake electronic supervision, a staff member appointed by the General Manager is to follow the procedures outlined under the heading *Offender Computer Security Check* (below). This staff member must at the same time also undertake a physical check of computer hardware for signs of tampering and ensure that all cables are connected to the correct ports (see 'Supervision' above).

The monthly check should be notified to the Manager Security for recording in their journal.

The shadowing function available as part of the *Offender Citrix Environment* is also available to supervising staff to covertly follow an inmate's work in real time. Staff should avoid reading any documentation that relates to an inmate's legal proceedings as this information may be claimed by the inmate to be privileged.

5.4.6. Network printers – CSI workplaces

All cabling into network printers must be checked prior to an inmate commencing duties in CSI workplaces to ensure that it is plugged into the correct port. At the cessation of duty, the cabling must also be checked.

Within CSI workplaces, inmates are not to be seated near network printers or permitted to use such printers if the inmate cannot be directly physically supervised in its use by an Industries or Correctional officer.

5.4.7. Software

5.4.7.1. Inmate purchase of software

Inmates undertaking courses of study may require the purchase or possession of computer software.

Software either issued or purchased must be relevant to the course or study being undertaken. Applications to acquire software must be endorsed by SCEO's and approved by the General Manager.

The purchase of the software must be done on the inmate's behalf by the SCEO or other officer appointed by the General Manager. Inmates are not permitted to have any software purchased privately and sent into a correctional centre.

Before purchasing any software, a check must be made with the IC & T Division by the SCEO or other officer to confirm the supplier is approved.

No maximum limit is prescribed in respect of purchase of software, however, the inmate property policy will apply in terms of the amount of private property inmates may keep. Any software purchased for the inmate is to be placed in the inmate's private property, once it has been loaded onto a computer for use by the inmate and the inmate's property module noted on OIMS (including the serial no. of the software).

Software must not be kept by the inmate in their cell. However, the inmate may retain the user manual. If the software needs to be regularly used, it may be retained by the SCEO to be loaded as required. It must be secured by the SCEO when not being used to guard against theft.

CSNSW has a legal obligation to ensure that all software installed on AEVTI/CSI controlled computers has been both legitimately purchased and correctly installed (i.e. no pirated software and all installed software must be licensed), and that there is compliance with copyright laws at all times. As stated below, software on an OAC Network will be installed centrally.

5.4.7.2. Software register

To ensure compliance, the SCEO (delegate) must maintain a *Software Register* containing the following information:

- the date and source of software requisition;
- details of licence;
- location of installation including serial number of the hardware in which each copy of the software has been installed (if non OAC network);
- the existence, location and number of backup copies; and
- the key (code) needed to be entered in order to activate the software.

The software configuration for each desktop computer is to match the details in the software register (non OAC network).

As part of carrying out the monthly check (as above) the software contained on each computer's hard drive must be matched against the details recorded in the software register as well as the software list outlined below - *Supervision of inmate access to computers (non OAC network)*.

5.4.7.3. Software - OAC Network

Software purchased for an inmate to be installed on the inmate's OAC account should be recorded within the *Software Register*.

On the OAC Network, software will be installed centrally to an inmate account by CSNSW Information Communication and Technology (IC&T) staff following its approval by SCEO/AEVTI, instead of being installed by staff at the centre where the inmate is located.

Following receipt of the software, it should be entered into the *Software Register* as above and then forwarded with a covering letter indicating approval of the software and the name and MIN number of the inmate to:

Assistant Commissioner
EA & CIO
CSNSW
Level 4 Henry Deane Building
20 Lee Street
SYDNEY NSW 2000

The software, after being installed, will then be returned to the centre to be placed in the inmate's property in the reception room as it will be available to the inmate through their OAC user account. The inmate's property module on OIMS should also be noted, upon return of the software.

5.4.8. Disks

5.4.8.1. Inmate disk register

During the course of approved computer-assisted educational and vocational training or to prepare legal documentation, it may be necessary to issue inmates with a floppy disk to save their work on ('inmate disk'). Whilst the OAC Network allows an inmate to save data to their 'My Documents' folder, in the event that the PC has not been logged into an inmate account or is a stand-alone PC, not part of the OAC Network, data will need to be saved to a floppy disk if it is to be retained.

Each disk used by an inmate is to be labelled with the inmate's name and MIN number and recorded in an *inmate disk* register by the officer issuing the disk.

Disks supplied with distance learning courses, as well as disks issued by correctional education officers to inmates for their use, must also be recorded in this register.

Under IC & T policy, inmates are not to possess or be supplied with USB memory sticks or hard drives on which to save data.

The transfer of inmate disks by inmates between the correctional centre and the community is prohibited unless in accordance with a distance education/external education program as detailed in the procedures below.

If an inmate is transferred to another centre, the Education Officer will make arrangements to forward the inmate's work disk to the education officer at the receiving centre. The education officer receiving the disk should inspect the contents and enter the disk on the *inmate disk register* at that centre.

Supervising staff must ensure that inmate disks issued are returned and accounted for at the end of each class / training session / working day. The disks must be securely stored. Inmates are not to set passwords for the disks.

5.4.8.2. Distance Education/External Education programs

There will be occasions when an inmate (students) will be required to forward inmate disks containing assignments to their distance learning institution. This should be verified by SCEO's with the institution prior to sending out.

SCEO's are to also check each inmate disk prior to its dispatch and note its transfer out of the correctional centre in the *inmate disk register*. It is preferable that these disks are not returned to the centre, but if it is, the SCEO is to make a note of its return in the *inmate disk register* and check its contents prior to reissuing the disk to the inmate.

There will also be occasions when an inmate (students) will be forwarded course material on an external storage device (e.g. CD, DVD, USB flash drive). The SCEO will arrange for the course material to be loaded on to a computer for the use of the inmate. The SCEO will then supply the external storage device to the Inmate Private Property Store where it will be stored. The OIC Inmate Private Property Store will record details of the external storage device in the OIMS inmate private property module.

5.4.9. Transfer of data between PC's being used by staff and those being used by inmates

Many staff computers no longer have a disk drive and as a result Education Officers and CSI Overseers are no longer able to transfer data onto and from PC's being used by inmates through use of a floppy disk.

In these circumstances, the use of a USB storage device by the staff member is permissible, provided the USB storage device always remains in the possession of the staff member and is not to be given to an inmate.

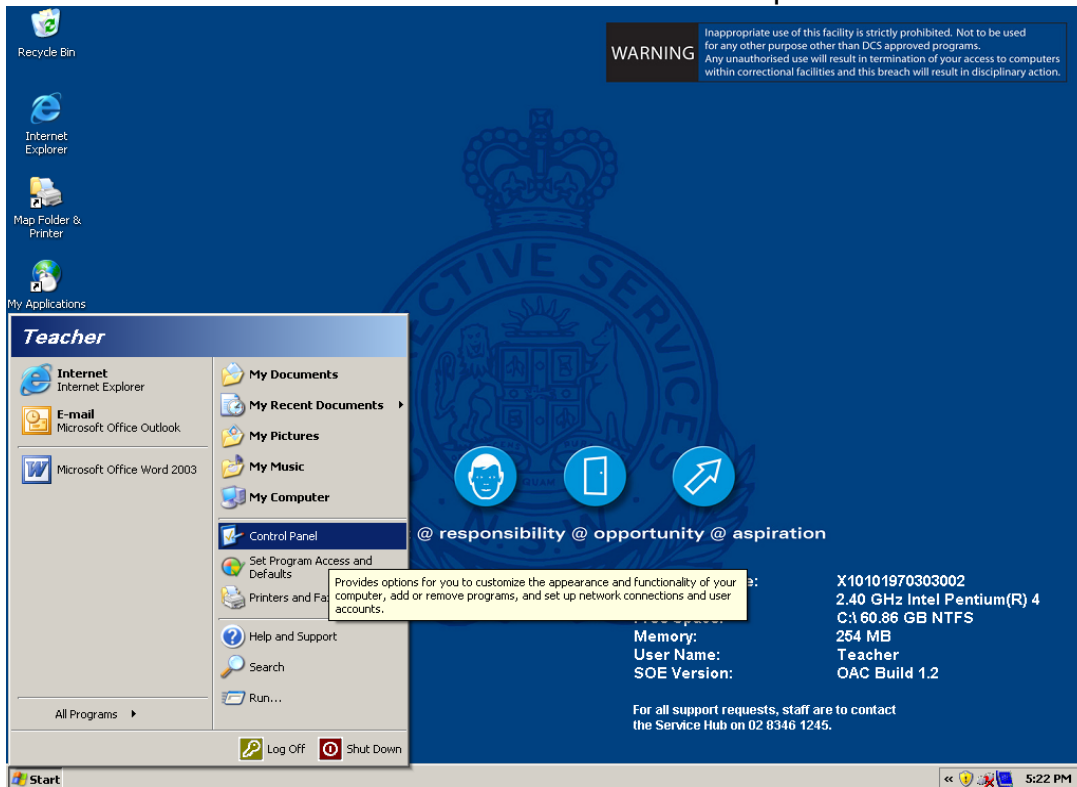
When an inmate's data has been put onto the staff computer by the staff member, it is able to be emailed to the relevant educational institution as required, obviating the need for a floppy disk.

5.4.10. Reporting of infringements

Correctional staff must report any infringement or non-compliance of this policy to the Senior Correctional Education Officer (SCEO) and Manager Security. Inmates found to be in breach of the '*Guidelines for Offenders Using Computers*' (Annexure 5.6) (or their employee contract) must have their access to computers withdrawn immediately pending determination of the allegation.

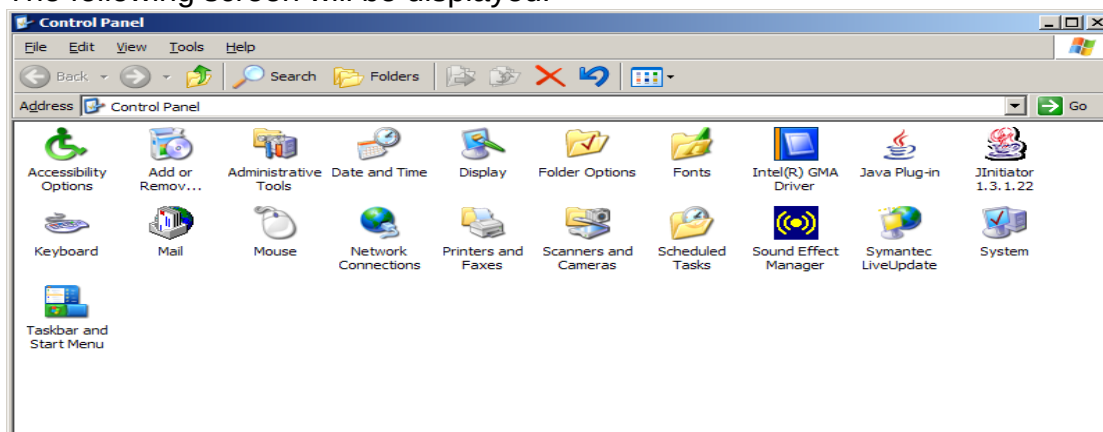
OFFENDER COMPUTER SECURITY CHECK

To check software installed on non OAC Network computer:-



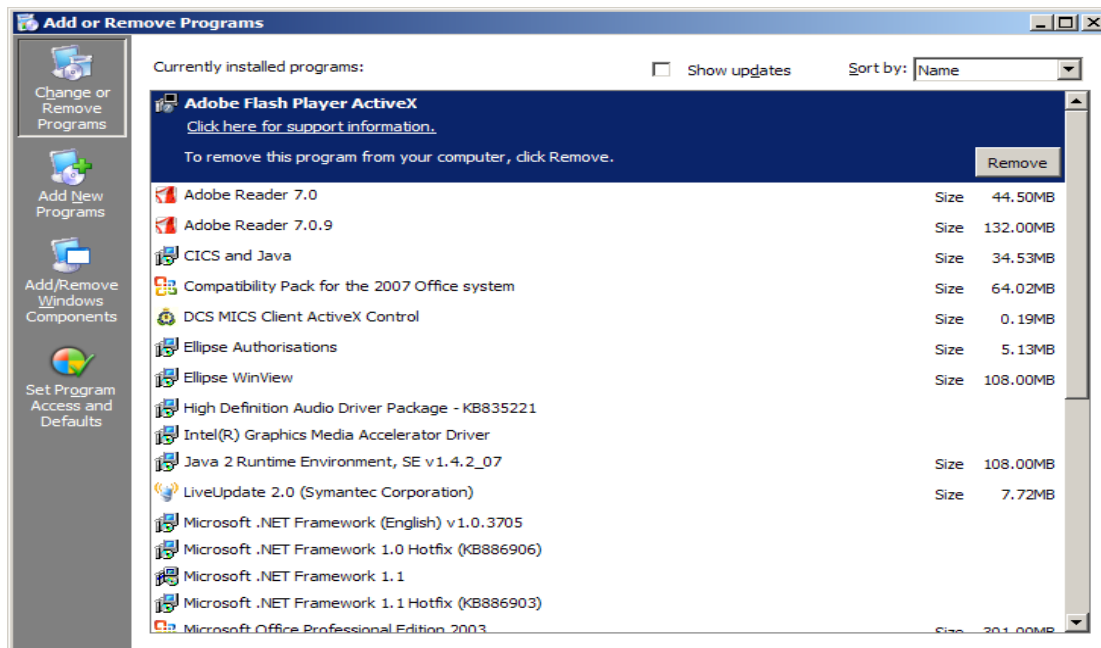
Click on the START button, select SETTINGS, select CONTROL PANEL

The following screen will be displayed:



Double click on the icon marked 'Add or Remove programs'

The following screen will be displayed:



Ensure that only the following CSNSW authorised programs are installed on the computer:

- Symantec Antivirus 10.1
- Microsoft.NET Framework 2.0
- Sun Java
- Microsoft Media Player 10
- Adobe Reader 7
- Macromedia Shockwave Player 8
- Macromedia Flash Player 8
- Microsoft Office 2003 Standard Edition
- Microsoft Word 2003
- Microsoft Excel 2003
- Microsoft PowerPoint 2003
- Microsoft Access 2003
- Microsoft Office 2003 Service Pack 2
- Apple Quick Time 5
- Typequick Student Edition
- Typequick Professional Edition
- Protea Issues in English 1
- Protea Issues in English 2
- Protea CGEA
- Protea Measuring Up
- Moorditj
- CSI Hygiene Operations 1
- Win XP SP 3
- Update to Anti-virus definitions

As well as any software shown in the software register as being installed on an inmate account

Reviewed	December 2011	Review Date	December 2013
-----------------	---------------	--------------------	---------------

DOCUMENT HISTORY

Version	Date	Reference
1.0	March 2005	As per Commissioner's Memo 2005/14
1.1	27 September 2006	Amendments as per DCOMO 2006/031
1.2	12 December 2006	Amendments to 5.4.1.1 as per DCOMO 2006/055
2.0	23 February 2012	Review of policy as per DCOMO 2012/26 and COPM 2012/17